DOC IT Security Evaluation Checklist: IT Security Officer Responsibilities

Appointed by the OU CIO, the OU ITSO serves as the central point of contact for the operating unit's overall IT Security Program. The OU ITSO reports on IT security program matters to the DOC IT Security Program Manager, through the OU CIO. An ITSO is the individual responsible for ensuring the appropriate operational security posture is maintained for information systems and programs under their operating unit's control. The ITSO serves as the principal advisor to the authorizing official, system owner, and DOC IT security program manager on all matters (technical and otherwise) involving the security of the operating unit's IT systems, and maintains a copy of each Security Accreditation Package (SAP) for use in performing required IT security monitoring and reporting responsibilities.

This checklist provides ITSOs with a self-assessment tool, and their supervisors with a performance evaluation tool, to evaluate the level of compliance with ITSO duties as established by the *DOC IT Security Program Policy and Minimum Implementation Standards (ITSPP) Section 2.1.8,* as well as the additional sections of the ITSPP cited in the second column of the checklist.

This is an assessment of (name/operating unit/office)**:**		
	Self Assessment	**Assessment Date:**
	Third Party Evaluation	**Assessor** (name/title/org.):

Status Codes: **1** = Not Started **2** = In Process **3** = In Place

Performance Levels:

1 ITSO has comprehensive IT security policies in place

2 ITSO has comprehensive IT security policies as well as detailed procedures in place

3 ITSO has comprehensive IT security policies and detailed procedures in place that are fully implemented for the operating unit's IT security program

4 ITSO has fully implemented and tested comprehensive IT security policies and detailed procedures in place

5 ITSO has fully implemented and tested comprehensive IT security policies and detailed procedures in place as part of a fully integrated IT security program

IT Security Officer (ITSO) Responsibilities		**ITSPP Section Reference***	**Status**	**Performance Level**
1	Develop and maintain operating unit IT security policy, procedures, standards, and guidance consistent with Departmental and federal requirements.			
2	Ensure the conduct of reviews to ensure that all systems have effective, quality IT security documentation in place, including:			
	(a) Qualitative risk assessments that conform to NIST SP 800-30;	3		
	(b) Current and effective IT security plans that conform to NIST SP 800-18 and are integrated into all stages of the system life cycle;	4.3		
	(c) Annual system self-assessments that conform to NIST SP 800-26 guidance;	6.3.1		
	(d) Current and tested contingency plans that conform to NIST SP 800-34; and	9		
	(e) Current certification and accreditation that conforms to NIST SP 800-53, 800-37.	6		

* In addition to Section 2.1.8

	IT Security Officer (ITSO) Responsibilities	ITSPP Section Reference*	Status	Performance Level
3	Conduct self-assessments of the operating unit's IT Security Program that conform with SP 800-26 annually to ensure operating unit effective implementation of and compliance with established policies and procedures;	6.3.1		
4	Establish a process to track remedial actions to mitigate risks in accordance with the DOC standard for plans of action and milestones (POA&Ms).	Appendix E		
5	Maintain the IT system inventory in accordance with the DOC standard for inventory management	Appendix F		
6	Establish a process to ensure that all users (including the ITSO) receive periodic IT security awareness briefings and copies of rules of behavior, are trained to fulfill their IT security responsibilities, and understand the consequences of non-compliance.	15.3, 6.3.1.3		
	(a) Develop procedures for an IT security awareness and training program for all operating unit personnel, including specialized training as necessary for system administrators, ITSOs, Contracting Officer's Technical Representatives (COTRs), etc.	15.4		
7	Act as the operating unit's central point of contact for all incidents, develop incident handling procedures, and report all incidents to the responsible incident response capability.	14		
8	Participate as a voting member of the DOC IT Security Coordinating Committee (ITSCC), participate in special committees under the ITSCC, and provide other support for the ITSCC as appropriate.	2.2.1		
9	Coordinate with the DOC IT Security Program Manager and CIPM, as well as OSY and OIG as appropriate on IT security matters (concerning incidents, potential threats, and other concerns).	2.1.3, 2.1.4, 20.3, 20.6		
10	Ensure that system owners establish processes to ensure:			
	(a) IT personnel are provided specialized training			
	(b) Access privileges are revoked in a timely manner (e.g. transfer, resignation, retirement, change of job description, etc.) – immediately for individuals being separated for adverse reasons on or just prior to notifying them of the pending action.	17		
11	Serve as certification agent for systems within their operating unit (except in the case of all systems for which the ITSO is also the system owner as well as moderate and high impact systems for which the ITSO is also the ISSO).	6		
12	Establish a process to identify, track, and report on security patch management.	10.4.1		
13	Establish a Chain of Custody that documents (in writing) the name, title, office, and phone number of each individual having sequential possession of a system's hard drive when it is removed due to compromise and the need for possible forensic examination of evidence for potential prosecution.	14.7.5		
14	Ensure that cryptography is used for transmission of classified national security information, in accordance with the DOC Security Manual, Chapter 22	16.8		
15	Ensure that IT security is addressed in the development and acquisition process of information systems and security related products and services by:			
	(a) Following a methodology consistent with NIST 800-64, Security Considerations in the Information System Development Life Cycle;	5.2.1		
	(b) Working with OU system owners to determine the information type and system impact levels and to determine the control baseline for protection of the system and its data;	5.4.1.2, 3.4.1, 1.7,		

	IT Security Officer (ITSO) Responsibilities	ITSPP Section Reference*	Status	Performance Level
	(c) Working with OU system owners to ensure integration of the system security configuration to the OU's security architecture, and the OU's architecture with the overarching DOC IT Enterprise Architecture (EA).	5.4.1.2		
16	Ensure that network and system warning banners communicate that there is no expectation of privacy in the authorized or unauthorized use of DOC IT systems.	4.5.4		
17	Ensure that OU policies and practices allow for the following account management controls:	17.3.1		
	(a) Account creation subsequent to request and authorization by supervisor;			
	(b) Identification and documentation of the user and appropriate access levels/account permissions;			
	(c) Account termination;			
	(d) Periodic status review of all currently open accounts on all systems through auditing (review) of user accounts (federal employee, contractor, and "guest" accounts).			